CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

ERNEST KOSCHINEG
ekoschineg@c-wlaw.com

JASON MICHAEL GOODWIN
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

Visit us online at
www.C-WLAW.com

March 30, 2022

Via Electronic Mail
Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202
IDTheft@oag.state.md.us

RE: Security Incident Notification

To Whom It May Concern:

We serve as counsel for BKA Financial, LLC. ("BKA Financial") located at 244 West Water St, Ste 200, Elmira, NY 14901 and provide this notification to you of a recent data security incident. By providing this notice, BKA Financial does not waive any rights or defenses under Maryland law, including the data breach notification statute.

BKA Financial recently discovered suspicious activity related to one employee email account. Upon discovery, BKA Financial took swift action to secure its email system and network. BKA Financial also launched an internal investigation and engaged leading, independent cybersecurity specialists. Based on this investigation, BKA Financial confirmed that one employee email account was subject to unauthorized access from January 22-25, 2022. As part of this process, BKA Financial investigated whether any sensitive information may have been at risk, and if so, to whom such information relates. Ultimately, it was discovered that information containing the name and driver's license number of one Maryland resident was subject to unauthorized access.

On March 31, 2022, BKA Financial is providing written notice of this incident to the Maryland resident pursuant to Maryland law. The notice letter includes an offer of complimentary credit monitoring and identity protection services offered through TransUnion for 12 months. A copy of the notice letter is attached hereto. BKA Financial also continues to review its policies and procedures related to data security.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: ______________________
Ernest Koschineg, Esq.

244 West Water St.; STE 200
Elmira, NY 14901

March 30, 2022

Name
Address
United States

Dear Name:

We are writing to inform you of a data security incident experienced by our company that involved your information as described below. We take the privacy and security of all information very seriously, and while we have no evidence to suggest that any information was subject to actual or attempted misuse as a result of this incident, this letter includes information about the incident and steps you can take to help protect your information, should you feel it appropriate to do so.

We discovered suspicious activity related to an employee email account, and upon discovery, took swift action to secure our email system and network. We also launched an internal investigation and engaged leading, independent cybersecurity specialists. Based on this investigation, we discovered that an unauthorized individual may have downloaded a file from the BKA sytem. Upon discovery, we performed a review of the file and learned that it contained an image of your driver's license, including your name, date of birth and driver's license number.

We have taken the steps necessary to address the incident, including the implementation of additional technical safeguards, and are committed to fully protecting all of the information in our care. Additionally, while we have no evidence that this information has been or will be misused, we are offering you complimentary credit monitoring and identity protection services. In an abundance of caution, our third-party specialists performed an extensive investigation, including a darknet scan, and identified no information associated with this incident.

In an abundance of caution, we recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft.

Should you have any question or concerns, please contact us at jbaker@bkafinancial.com or (607) 735-2378. The security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support.

Sincerely,

Johnnie Baker
Chief Information Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

TransUnion® *my*TrueIdentity provides you with the following key features:

- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- 12 months of unlimited access to your TransUnion® credit report and and VantageScore® credit score by TransUnion.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible.[1]

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code ***CODE*** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **697871** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **July 31, 2022**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your online credit monitoring benefits, need help with your enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);

---

[1] (Policy limitations and exclusions may apply.)

2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion	**Experian**	**Equifax**
1-800-680-7289	1-888-397-3742	1-888-298-0045
www.transunion.com	www.experian.com	www.equifax.com
TransUnion Fraud Alert	**Experian Fraud Alert**	**Equifax Fraud Alert**
P.O. Box 2000	P.O. Box 9554	P.O. Box 105069
Chester, PA 19016-2000	Allen, TX 75013	Atlanta, GA 30348-5069
TransUnion Credit Freeze	**Experian Credit Freeze**	**Equifax Credit Freeze**
P.O. Box 160	P.O. Box 9554	P.O. Box 105788
Woodlyn, PA 19094	Allen, TX 75013	Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. BKA Financial may be contacted at 244 West Water St, Ste 200, Elmira, NY 14901.